



**U.S. Department of Justice**

*United States Attorney  
Eastern District of New York*

CRH:AFM/JAM  
F. #2021R00874

*271 Cadman Plaza East  
Brooklyn, New York 11201*

June 3, 2024

By ECF

The Honorable Eric N. Vitaliano  
United States District Court  
Eastern District of New York  
225 Cadman Plaza East  
Brooklyn, New York 11201

Re: United States v. Anatoly Legkodymov  
Criminal Docket No. 23-496 (ENV)

Dear Judge Vitaliano:

The government respectfully submits this sentencing memorandum in advance of defendant Anatoly Legkodymov's sentencing hearing, which is scheduled for June 28, 2024 at 2:30 p.m. As set forth below, the applicable range under the United States Sentencing Guidelines ("Guidelines") is 60 months' imprisonment. The government submits that a sentence slightly below the Guidelines—between 48 and 60 months—is appropriate for reasons further discussed below.

I. Introduction

For six years, Anatoly Legkodymov owned and controlled Bitzlato, a financial institution whose only selling points were its amenability to fake accounts and a "no questions" asked policy about customer identity. During that time, he was repeatedly told that Bitzlato had become a haven for criminals: drug dealers, ransomware extortionists, and dark-web sellers of forged identity documents and stolen financial information. All of these players in the criminal ecosystem used Bitzlato as a platform through which they could anonymously exchange fiat currency for cryptocurrency, and vice versa.

Most notably, Bitzlato was the largest counterparty of Hydra Market, a notorious dark web market that was ultimately shut down through coordinated international law enforcement action. Bitzlato users directly exchanged more than \$290 million worth of cryptocurrency with Hydra Market. When transactions through intermediaries are counted as well, the total volume of funds exchanged exceeded \$700 million worth of cryptocurrency. Presentence Investigation Report prepared on February 6, 2024 ("PSR") ¶¶ 7-8.

In addition to these transactions with Hydra Market, ransomware<sup>1</sup> criminals used Bitzlato to launder the cryptocurrency paid by their extortion victims. Ransomware actors under investigation by the FBI have funneled more than \$1.2 million worth of cryptocurrency through accounts on Bitzlato. That figure necessarily undercounts the true total, because it is limited to FBI-investigated cases in which case agents happen to be aware that funds moved through Bitzlato.<sup>2</sup>

The defendant knew all this. As early as 2018, he joked with a colleague about the integral role played by drug dealers in Bitzlato. Months later, in April 2019, he was warned that “Bitzlato clients are addicts who buy drugs at the hydra site.” In May of 2019, he described Bitzlato’s users as “crooks” who signed up with fake identities. By October 2021, the defendant acknowledged that Bitzlato’s critics were “right about Hydra.” And four months later, faced with a critical report from the blockchain analytics firm Chainalysis, the defendant asked a subordinate to investigate using Bitzlato’s own compliance platform. He then wrote to a colleague: “It turns out that we have at least 20% dirt. And in this situation I don’t see any reason to fight with Chainalysis.”

Bitzlato’s pipeline for turning cryptocurrency into cash enabled ransomware actors to attack American businesses, criminals to sell forged U.S. passports and stolen financial information, and drug dealers to sell millions of dollars’ worth of narcotics. Rather than fix the company or shut it down, the defendant continued to operate Bitzlato and so perpetuated its harms. That is why he comes before this Court for sentencing.

A substantial sentence, in the range of 48-60 months, is warranted to recognize the severity of the defendant’s conduct and the harm done by lawless financial institutions.

## II. Factual Background

The defendant was Bitzlato’s founder, majority owner, and seniormost executive. PSR ¶ 5. He sat atop the company’s organizational chart, alongside his co-founder (“Executive-1”). See Exh. A (redacted organizational charts, in the original Russian and in English translation). He held and exercised final authority within the organization. And he was repeatedly informed, as set forth below, that Bitzlato was processing a high volume of illicit funds.

This section of the government’s submission first addresses the evidence showing that Bitzlato’s employees were aware of illicit transactions, and then discusses the evidence that the defendant himself knew of those transactions.

---

<sup>1</sup> Ransomware is a form of extortion whereby attackers break into a victim’s computer system and encrypt the files so that they are no longer readable by the victims. The attackers then demand payment in exchange for a decryption key. The payment demanded is typically in the form of cryptocurrency.

<sup>2</sup> A commercial blockchain analysis firm has estimated the volume of ransomware proceeds flowing through Bitzlato at \$15 million. PSR ¶ 11.

#### A. Knowledge of Illicit Transactions by Bitzlato Employees

Bitzlato’s employees were specifically aware of the platform’s transactions with Hydra, because many users wrote to its customer-service personnel asking for help transferring funds to or from Hydra. Bitzlato customer service employees sometimes refused to help and/or blocked these users, but on numerous other occasions they facilitated these transactions. For example, Bitzlato employees assisted a user who said he wanted to “exchange dirty bitcoin . . . from [the] darknet,” and another who wrote that he intended to purchase “opiates on Hydra.” Mere days before Hydra Market was shut down by international law enforcement, Bitzlato employees assisted a customer who indicated explicitly that he wanted to send funds to Hydra, giving him instructions for the transaction. Numerous other examples are cited in the PSR. PSR ¶ 15.

Bitzlato’s customer service personnel were also aware that many customers were using accounts opened by others (“drop” accounts, in Russian slang) and carrying out straw transactions. Bitzlato did not consistently penalize such customers and, in fact, had a practice of accepting straw credentials as validation for accounts. To take two examples among the many cited in the PSR:

- On or about May 7, 2022, a Bitzlato user was asked to provide his identifying information. The user responded that he was “not going to lie to you and tell you tales[.] I bought this account—bought it, I’m telling you.” The user added that there were “hundreds of these accounts with passed verifications—as if you didn’t know that.” The user offered to “find the man” whose credentials had been used to verify the account, and “pay him to send everything you need, because the money is mine.” The Bitzlato representative responded: “That’s your right.”
- On or about September 12, 2022, Bitzlato blocked a user’s account and asked him to verify his identity. The user responded that he would provide “a woman’s” identity documents, adding: “Am I an idiot to verify myself? Verify the ‘drop.’” The user added that he would be transferring ransomware proceeds and “a payment from Hydra” to his Bitzlato account. The Bitzlato customer service representative responded that an account verified in the name of the user’s “drop,” or straw man, would “belong to your drop,” and concluded: “Okay, we are waiting for the application.”

PSR ¶ 16.

#### B. The Defendant’s Knowledge of Illicit Transactions

The information described above – that Bitzlato was riddled with “drop” accounts and that it was the first stop for illicit funds flowing into and out of Hydra—did not remain trapped at the level of Bitzlato’s customer service employees. It made its way to the company’s highest echelon, where the defendant sat. Numerous seized chats between the defendant and his senior executives show his awareness that a high volume of criminal proceeds flowed through Bitzlato.

Moreover, the defendant's knowledge of illicit transactions running through Bitzlato did not develop slowly over time. Rather, he knew from the start that Bitzlato was heavily used by criminals. And although the defendant made a practice of voicing passive opposition to this fact, he never changed it, nor did he sell Bitzlato or otherwise withdraw from the company.

#### 1. The Defendant's Knowledge in 2018-2019

Examples of the defendant's communications evincing knowledge of illicit transactions in 2018-2019 are set forth below:

- In October 2018, the defendant's partner and cofounder ("Executive-1") reported to the defendant that Bitzlato had been abandoned by "small-time dealers" who had been "scared off by the drug war." Executive-1 advocated taking a "nominal" approach to "the fight against drug traffickers" – "i.e., block once a month when [they] can clearly be found." The defendant in essence agreed, and advocated turning a blind eye to drug-related transactions by blocking only those transactions where the transacting parties made explicit reference to drugs, such as writing (in the defendant's jocular example) "'for cannabis.'" PSR ¶¶ 16-20. Executive-1 raised the possibility of resultant trouble with the police, and discussed with the defendant the possibility of moving Bitzlato to another jurisdiction. Executive-1 added that he did not want to move the company to Malta or England because "I don't want company in the asshole." At this point, the defendant proposed moving the conversation to a telephone call.
- On December 6, 2018 the defendant and Executive-1 discussed the then-recent news that Huawei executive Meng Wanzhou had been arrested in Canada pursuant to a request from the United States. Executive-1 wrote: "Fuck, we're all noncitizens of the U.S." The defendant responded: "We need an island armed to the teeth."
- On April 23, 2019, Executive-1 warned his colleagues, including the defendant, that "Bitzlato clients are addicts who buy drugs at the hydra site." The defendant responded with a proposal to expand Bitzlato's services to everyday individuals seeking privacy. PSR ¶¶ 21-22.
- On May 29, 2019, the defendant wrote to a colleague in a chat: "All traders are known to be crooks. Trading on 'drops,' etc. You do realize that they all (I think 90%) do not trade on their [identity] cards." Later that year, on or about June 22, 2019, the defendant commented: "Scammers know that it is possible to be verified for a drop and 100% withdraw money." PSR ¶¶ 23-24.

## 2. The Defendant's Knowledge in 2021-2022

As noted above, Bitzlato was the largest single counterparty of the notorious dark-web bazaar Hydra Market. Hydra was shut down through coordinated U.S and German law enforcement action on April 5, 2022, and the Department of Justice unsealed an indictment of Dmitry Olegovich Pavlov for conspiracy to distribute narcotics and conspiracy to commit money laundering, in connection with his operation and administration of the servers used to run Hydra. See Department of Justice, “Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace,” available at <https://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace>; United States v. Pavlov, 22-cr-143-CRB, Indictment (N.D. Cal. April 5, 2022) (the “Pavlov Indictment”).

The Pavlov Indictment alleges that buyers on Hydra Market could purchase customized U.S. passports or drivers’ licenses, as well as visas for the United States and Europe, and that Hydra users purchased narcotics from the United States and had them shipped to U.S. addresses. Pavlov Indictment ¶¶ 5, 22(a). Hydra vendors also sold hacking tools and services. Id. ¶ 6.

Beginning in 2021, the defendant increasingly evinced specific knowledge about Hydra Market and repeatedly acknowledged that Bitzlato was notorious for money laundering. For example, on October 6, 2021, the defendant asked his employees about Hydra Market in a chat and was sent a Russian-language Wikipedia article. A version of that article, as it appeared on October 26, 2021, is available through the Internet Archive, an online archiving project.<sup>3</sup> Its first sentence described Hydra Market as “the largest Russian darknet market for drug trafficking, the world’s largest resource in terms of the volume of illegal transactions with cryptocurrency.” The article further noted that “[i]n addition to drugs, popular products on Hydra are counterfeit money and documents, [and] instructions for illegal activities. The resource also provides services such as drug sales, Internet security and account hacking.”

Notably, the defendant repeatedly acknowledged that Bitzlato’s own data confirmed what third-party blockchain analysis platforms were saying: Bitzlato was processing a large volume of illicit transactions, and specifically transactions with Hydra Market. On October 19, 2021, for example, after hearing that industry personnel were accusing Bitzlato of cooperating with Hydra and facilitating drug transactions, the defendant wrote to his fellow senior executives: “On the one hand, they are right about Hydra. But on the other hand, [there are] 2.5 million Hydra users. Everyone is involved in it. This can’t be filtered out.”

On February 14, 2022, Chainalysis, a blockchain analysis firm, released the 2022 version of its annual “Crypto Crime Report,” which reported that Bitzlato users had received

---

<sup>3</sup> Available at [https://web.archive.org/web/20211026044000/https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%B4%D1%80%D0%B0\\_\(%D0%B4%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82-%D1%80%D1%8B%D0%BD%D0%BE%D0%BA\)](https://web.archive.org/web/20211026044000/https://ru.wikipedia.org/wiki/%D0%93%D0%B8%D0%B4%D1%80%D0%B0_(%D0%B4%D0%B0%D1%80%D0%BA%D0%BD%D0%B5%D1%82-%D1%80%D1%8B%D0%BD%D0%BE%D0%BA))

\$206 million from darknet markets, and \$9 million from ransomware attackers.<sup>4</sup> The defendant inquired with a subordinate, who shared the below graphic with him on February 25, 2022—apparently a screenshot from Bitzlato’s own transaction screening software:<sup>5</sup>

count	transaction_entity_name
403119	NULL
10	"SatoshiMines.com"
2	"BitZino.com"
546	"Wasabi"
76159	"Hydra Market"

The defendant and his colleagues subsequently determined that over the past three months, 20% of the transactions from Bitzlato had sent funds to Hydra Market. “Withdrawals to Hydra?” the defendant wrote. “More than 20%? . . . Let’s clean everything down to zero, ASAP.”

Later that day, the defendant wrote to a colleague: “It turns out that we have at least 20% dirt. And in this situation I don’t see any reason to fight with Chainalysis.” On February 18, 2022, the defendant wrote to Executive-1 to complain that his executives were ruining Bitzlato’s acquisition value by laundering money: “Who am I (we) going to sell Bitzlato to now with such a report from chainalysis[?] And this is 90% due to management rather than us.” One week later, on February 25, 2022, the defendant wrote to Executive-1: “I did some hard thinking. I can’t get over 20% dirt and being totally ignored, and I want to close the company. . . . You are not supporting me in getting rid of dirt. We don’t have a plan, but you are claiming that you either have no support or something else. I am not interested in continuing under such conditions. I want to close the company and start something else with a blank slate.” The next day he added: “You are all throwing me under the bus. 76,000 transactions with Hydra and no interest at all.”

Approximately two months later, on April 7, 2022, the defendant criticized his compliance personnel for failing to investigate their own exposure to illicit funds, using the tools at their disposal (such as the compliance vendor Valega, see Deft. Mem. 11). “You still haven’t figured out how many transfers we’ve had to dark markets in the last three months (according to Valega)” he wrote. “This ignorance is alarming.” On April 10, 2022, a compliance executive reported to the defendant that over the preceding six months, out of 76,000 active users, 27,000 had attempted to transfer funds to or from what the employee termed “dirty” cryptocurrency

---

<sup>4</sup> Available at <https://go.chainalysis.com/rs/503-FAP-074/images/Crypto-Crime-Report-2022.pdf>

<sup>5</sup> “Wasabi” likely refers to Wasabi Wallet, a Bitcoin “mixer” that is used to obscure cryptocurrency transactions from scrutiny on the blockchain. Among other high-profile crimes, Wasabi Wallet has been used to launder millions of dollars’ worth of proceeds from computer intrusions and exploits committed against cryptocurrency exchanges.



addresses. Another employee commented in the same chat: “It’s just that services with a low AML level are very convenient for [money] launderers. As soon as we implement all AML/KYC tools, the number of dirty transactions will decrease significantly.”

The defendant and his colleagues repeatedly voiced their awareness that operating Bitzlato could place them in legal jeopardy. For example, Executive-1’s October 2018 comment about “company in the asshole” appears to have been a reference by to the prospect of facing time in prison. On April 6, 2022, after Hydra Market was taken down through international law enforcement action, the defendant commented that “[w]e are next in line unless we clean out all the dirt.”

By the fall of 2022, when the defendant traveled to the United States, he appears to have been serving as Bitzlato’s acting CEO. A communication from the defendant to his fellow senior executives on November 11, 2022 captures the extent of his involvement and authority. “Basically,” he wrote, “I am getting a clear understanding of where the trouble is and what to do. . . . Over this week, I (as CEO)<sup>6</sup> figured out that I personally didn’t get along workwise with half of the staff (top management). Top management didn’t show results before I came in, [and] that’s why I will change half of the personnel if I remain CEO.”

As before, the defendant continued to call for improvements at Bitzlato, without making any real change. On November 7, 2022, for example, the defendant voiced his desire for more stringent KYC policies, voicing his view that “over decades of experience, I’ve become convinced that 95% of anonymous people are criminals.” A colleague responded that most of Bitzlato’s users were indeed criminals, asserting that small-time users were “the former USSR, the fans of dark resources[,] drug addicts, documents, and other dirt.” By contrast, the colleague said, higher-value users were “criminals, as you’ve said, but all the big guys are going to get ‘drops’ for their needs anyway.” The defendant responded that “just getting a bunch of druggies on the cheap means that the Marketing Department is slacking . . . this is the error which was made several years ago, and I don’t want to repeat it.”

### III. Procedural Background

The defendant was charged by complaint in the Eastern District of New York on January 6, 2023, and a warrant issued for his arrest. He was arrested on January 17, 2023 in Miami, Florida. The defendant waived indictment and pled guilty before Your Honor on December 6, 2023 to an information charging a single count of violating 18 U.S.C. § 1960(b)(1)(C), which prohibits operating a money transmitting business that “involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity.”

At the time of his guilty plea, the defendant acknowledged having “bec[o]me aware that Bitzlato was being used by some of its clients to receive and to transmit cryptocurrency that was derived from unlawful activity. Although we were making significant

---

<sup>6</sup> The defendant’s assertions about being the CEO of Bitzlato are in significant tension with his claim that he “was not the CEO of Bitzlato.” Deft. Mem. 15.

improvements to our Know Your Customer and anti-money laundering enforcement, I was aware that ransomware proceeds and many transactions associated with the Hydra Market were making their way into Bitzlato. I also understood that Bitzlato had clients who registered for their accounts using false or purchased identification data, including users receiving funds from individuals in the United States, including in the Eastern District of New York.”

Notably, the defendant’s guilty plea included the release of any claim over assets of Bitzlato seized by the French authorities in connection with a parallel criminal investigation.

[REDACTED]

#### IV. Applicable Law

The Supreme Court has instructed that a district court “should begin all sentencing proceedings by correctly calculating the applicable Guidelines range. As a matter of administration and to secure nationwide consistency, the Guidelines should be the starting point and the initial benchmark.” Gall v. United States, 552 U.S. 38, 49 (2007) (citation omitted).

Next, a sentencing court should “consider all of the § 3553(a) factors to determine whether they support the sentence requested by a party. In so doing, [it] may not presume that the Guidelines range is reasonable. [It] must make an individualized assessment based on the facts presented.” Id. at 50 (citation and footnote omitted). Title 18, United States Code, Section 3553(a) provides, in part, that in imposing a sentence, a court shall consider:

(1) the nature and circumstances of the offense and the history and characteristics of the defendant; [and]

(2) the need for the sentence imposed--

(A) to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense;

[REDACTED]



(B) to afford adequate deterrence to criminal conduct; [and]

(C) to protect the public from further crimes of the defendant.

Section 3553 also recognizes the need to afford the defendant opportunities for rehabilitation. See 18 U.S.C. § 3553(a)(2)(D). Thus, the Court must first calculate the correct Guidelines range, and then apply the 3553(a) factors to arrive at an appropriate sentence. The sentencing court must also “remain cognizant of them throughout the sentencing process.” Gall, 552 U.S. at 50 n.6.

#### V. Guidelines Calculation

The government agrees with Probation’s calculation of the defendant’s offense level under the United States Sentencing Guidelines (“U.S.S.G. or “Guidelines”) as set forth below.

Base Offense Level (U.S.S.G. §§ 2S1.1(a)(2) and 2B1.1(b)(1)(P))	38
Plus: Knowledge that any of the laundered funds were proceeds of an offense involving the distribution of a controlled substance (U.S.S.G. § 2S1.1(b)(1)(B)(i))	+6
Plus: Defendant was in the business of laundering funds (U.S.S.G. § 2S1.1(b)(2)(C))	+4
Total:	48
Less: Acceptance of Responsibility (§§ 3E1.1(a), (b))	-3
Less: Adjustment for Certain Zero-Point Offenders (§ 4C1.1)	-2
Adjusted Total:	<u>43</u>

PSR ¶¶ 37-47.

The adjusted total offense level is 43, which, based on a criminal history category of I, corresponds to a Guidelines recommendation of life imprisonment. However, because the statutory maximum sentence for a violation of Section 1960 is 60 months’ imprisonment, the effective Guidelines recommendation in this case is a sentence of 60 months. Id. ¶ 76.

Much of the Defense Memorandum is devoted to an argument that the Probation Department’s Guidelines calculation is mistaken. See Deft. Mem. 18-35. The defendant argues that the true amount of money laundered by Bitzlato is impossible to calculate for Guidelines purposes and that, instead, the defendant’s profits should be used as the linchpin of the Guidelines calculation. Deft. Mem. 35. This argument is wrong, conceptually and legally. The Probation Department’s calculation of the Guidelines is correct and a Guidelines sentence in this case is 60 months, the statutory maximum.

A. The Enhancements for Laundering Drug Proceeds and Operating a Money Laundering Business Are Properly Applied

The defendant contests application of the enhancements for knowledge that any of the laundered funds were proceeds of a controlled-substance distribution offense (U.S.S.G. § 2S1.1(b)(1)(B)(i)) (the “Drug Proceeds Enhancement”) and for being in the business of laundering funds (U.S.S.G. § 2S1.1(b)(2)(C)) (the “Money Laundering Business Enhancement”). Deft. Mem. 30-32. Both enhancements squarely apply.

Application of the Drug Proceeds Enhancement is straightforward. It applies where the defendant “knew or believed that any of the laundered funds were the proceeds of, or were intended to promote [] an offense involving the manufacture, importation, or distribution of a controlled substance or a listed chemical.” The defendant repeatedly acknowledged his platform’s popularity with individuals looking to purchase drugs on the dark web. See, e.g., PSR ¶¶ 16-20 (discussing effect of “the drug war” on Bitzlato). He reviewed a Wikipedia article about Hydra Market, which described it as “the largest Russian darknet market for drug trafficking, [and] the world’s largest resource in terms of the volume of illegal transactions with cryptocurrency.” He reviewed figures showing the prevalence of Hydra-related traffic on Bitzlato. And he ruefully said, after Hydra was taken down, that “We are next in line unless we clean out all the dirt.” He cautioned his marketing department against “just getting a bunch of druggies on the cheap,” which he described as “the error which was made several years ago.”

The defendant attempts to deny this knowledge, arguing in conclusory fashion that he was not “involved in or knowledgeable of” the drug transactions that his platform was enabling, and contending that he did not “support them.” Deft. Mem. 30.<sup>8</sup> This argument is a red herring. The operative question is whether the defendant knew Bitzlato was transferring illicit funds, not whether he was pleased about the transactions, much less whether he was involved in them. Nor does Section 1960 require that the defendant have known about each transaction at an individual level. If that were so, a senior position in the organizational hierarchy would effectively shield a defendant from liability – yet Section 1960 by its terms prohibits “owning” or “controlling” an unlicensed money transmitting business.

Application of the Money Laundering Business Enhancement is also warranted. The defendant met four of the non-exhaustive considerations listed in the Guidelines. See U.S.S.G. § 2S1.1 cmt. 4(B). He regularly engaged in laundering funds because he ran Bitzlato for years. That laundering occurred over an extended period – the charged period from 2016 to 2022. PSR ¶ 2. The laundered funds came from “multiple sources”—to wit, Bitzlato’s tens of thousands of customers. And the defendant generated a substantial amount of revenue from Bitzlato’s laundering—enough to support a company with more than 60 employees, see Exh. A.

---

<sup>8</sup> With reference to the specific exchange recounted in PSR ¶¶ 16-20, the defendant argues that “junkies” is a mistranslation. Deft. Mem. 30. But that explanation is inconsistent with the defendant’s reference to “cannabis” in the same conversation and with Executive-1’s reference to the “drug war.”

The defendant contends that he was not “engaged” in laundering funds because (in his view) he merely ran a technological platform that might have enabled money laundering: “To the extent any funds were laundered, that action was committed by the underlying customer.” Deft. Mem. 31-32. But that argument elides Bitzlato’s role in these transactions. Bitzlato provided accounts that its customers could use to swap fiat currency for cryptocurrency. It had the ability to query its customers, to analyze their source and destination addresses, and even to freeze their accounts. Deft. Mem. 22. It was not a mere observer of this activity; it sponsored and enabled it.

The defendant’s argument that he is “not a crypto millionaire” further misses the point, conflating profit with revenue. Bitzlato employed scores of people, processed the equivalent of billions of dollars, and lasted nearly a decade; its revenue was “substantial,” regardless of its profits. Application of this Guideline reflects the Sentencing Commission’s insight that “defendants who routinely engage in laundering funds on behalf of others, and who gain financially from engaging in such transactions, warrant substantial additional punishment because they encourage the commission of additional criminal conduct.” Commentary n. 22 to Amendment of Guideline 2S1.1, at 156, available at [https://www.ussc.gov/sites/default/files/pdf/amendment-process/reader-friendly-amendments/20010501\\_RF\\_Amendments\\_0.pdf](https://www.ussc.gov/sites/default/files/pdf/amendment-process/reader-friendly-amendments/20010501_RF_Amendments_0.pdf).

The Money Laundering Business Enhancement and the Drug Proceeds Enhancement are both therefore properly incorporated into the Guidelines calculation for Bitzlato.

**B. A Guidelines Sentence Would be 60 Months Under Nearly Any Factual Scenario**

The Court need not find that the defendant laundered \$700 million in order to conclude that the Guidelines recommend a 60-month sentence. In fact, a Guidelines sentence in this case would be 60 months even if the defendant had laundered far less than \$700 million—indeed, even if the amount laundered was “only” \$550,000.

That is because the low statutory maximum sentence for the charged crime dramatically restricts the application of the money laundering guideline. By being charged with a violation of Section 1960 (and not with a money laundering charge pursuant to 18 U.S.C. § 1956) the defendant has avoided the full extent of the money laundering guidelines, which would otherwise counsel a much longer sentence.

For example, even if the Court were to find that the defendant laundered “only” \$550,000, the Guidelines would recommend a 60-month sentence, assuming applicability of the relevant enhancements (discussed above). In such a case, the defendant’s base offense level would be 22. See U.S.S.G. § 2S1.1(a)(2) (directing that the base offense level equal 8, plus the corresponding amount from the loss table in § 2B1.1(b)(1)). After application of the two enhancements discussed above, the defendant’s offense level would be 32. After reductions for acceptance of responsibility and for being a first-time offender, the defendant would have an adjusted total offense level of 27, corresponding to a theoretical Guidelines range of 70-87 months, which would be reduced to 60 months per the statutory maximum. Thus, even using a

small percentage of the tainted funds that flowed through Bitzlato, the defendant would still be facing the statutory maximum.

### C. The Defendant's Other Objections to the Guidelines Are Meritless

The defendant further argues that his Guidelines range should be lowered from Probation's estimate (1) in order to exclude funds that traveled through intermediaries as they passed between Bitzlato and Hydra Market, Deft. Mem. 20-21; (2) in order to exclude laundered funds reflecting crimes outside the United States, *id.* 22-26; and (3) to reflect his supposedly "minimal" role in operating Bitzlato, *id.* 33-34. None of these arguments has merit.

First, excluding transactions with "indirect" exposure (meaning transactions that passed through intermediary parties) would have no practical impact on the defendant's guidelines calculation, as Bitzlato users exchanged more than \$290 million worth of cryptocurrency directly with users of Hydra Market. PSR ¶¶ 9-10. For the reasons explained above, reducing the value of the amount laundered from \$700 million to \$290 million would not result in a reduction in the Guidelines sentence.

Second, excluding transactions outside the United States similarly would have no practical impact on the defendant's guidelines because the government has identified the equivalent of more than \$1.2 million that entered Bitzlato after being paid by U.S. victims of ransomware extortion. That amount, for the reasons set forth above, is more than sufficient for a Guidelines range exceeding the statutory maximum of 60 months. Moreover, Hydra Market was used to purchase forged U.S. identification documents, to order narcotics for shipment to the United States, and to procure services directed against U.S. victims.

In any event, the defendant is wrong on the law in contending that proceeds of foreign-law violations should be excluded from the Guidelines calculation under U.S.S.G. § 2S1.1 for a violation of 18 U.S.C. § 1960(b)(1)(C). He relies principally on the Second Circuit's holding in United States v. Azeem, 946 F.2d 13 (2d Cir. 1991), where the panel held that the weight of narcotics trafficked by the defendant from Pakistan to Egypt should not have been used in calculating the Guidelines range for his heroin trafficking sentence, because the foreign drug shipment "was not a crime against the United States." *Id.* at 16. But Azeem's holding is limited to prosecutions where the crime of conviction excludes overseas conduct. See United States v. Greer, 223 F.3d 41, 59 (2d Cir. 2000), opinion amended and superseded on other grounds, 285 F.3d 158 (2d Cir. 2002) (in prosecution under Maritime Drug Law Enforcement Act ("MDLEA"), distinguishing Azeem and upholding Guidelines consideration of drugs seized in Canada and intended for distribution in Canada, because "the crimes in this case are not foreign crimes; the MDLEA is a United States criminal statute that specifically covers conduct outside the United States"); *cf.* Carrasco v. United States, 820 F. Supp. 2d 562, 568 (S.D.N.Y. 2011) ("[T]he Sentencing Guidelines require a court to consider all of a defendant's conduct that was related to the offense, even where that conduct occurred outside the United States. . . . [C]onduct justifying enhancements under the Guidelines is in no way limited to conduct that occurred within the territorial United States.").

Section 1960(b)(1)(C)'s reach, like that of the MDLEA discussed in Greer, covers foreign activity. It broadly reaches the transfer of funds "known to the defendant to have been

derived from a criminal offense or [] intended to be used to promote or support unlawful activity.” The term “unlawful activity,” undefined in Section 1960, is addressed in Section 1956(c)(1):

the term “knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity” means that the person knew the property involved in the transaction represented proceeds from some form, though not necessarily which form, of activity that constitutes a felony under State, Federal, or foreign law[.]

18 U.S.C. § 1956(c)(1) (emphasis added). Because Section 1960(b)(1)(C) reaches the transfer of funds that stem from, or are destined to support, foreign-law crimes, the Guidelines analysis in this case properly encompasses funds associated with the worldwide purchase and sale of stolen financial information, forged credentials, hacking services and narcotics through Hydra Market.

The defendant’s argument for a mitigating role reduction, Deft. Mem. 33-34, is similarly meritless. The defendant seeks a four-point minimal role reduction, a designation that is reserved under the Guidelines for individuals “who are plainly among the least culpable of those involved in the conduct of a group.” U.S.S.G. § 3B1.2 cmt n.4.

The reduction on its face does not apply to the defendant. Section 1960 punishes, in relevant part, one who “controls . . . directs, or owns all or part of” a money transmitting business that involves the transmission of illicit funds. The defendant sat atop Bitzlato’s organizational hierarchy and, as such, is the *most* culpable individual, not the least. Audaciously, the defendant attempts to shift responsibility for his conduct onto Bitzlato’s users, arguing that “the customers on the exchange were the bad actors.” Deft. Mem. 33. But that argument mistakes the crime at issue. Section 1960 by its terms criminalizes “owning” and “controlling” a business that engages in the prohibited conduct. Bitzlato’s users do not own or control the platform and have no relevant criminal liability under Section 1960.

## VI. Discussion

### A. A Substantial Sentence Near the Statutory Maximum is Appropriate

Criminal actors tend to accumulate cryptocurrency, but there are few ways to anonymously turn cryptocurrency into cash: legitimate financial institutions across the world require that their clients identify themselves, and closely scrutinize the information they provide. That makes those institutions unappealing to criminals, who can expect to be pursued by investigators following the money. Into this gap came Bitzlato, led by Anatoly Legkodymov. Under the defendant’s leadership and with his full awareness, Bitzlato became an interface between the legitimate financial system and the dark web, serving as a jumping-off point for funds paid into dark markets, and an early stop for ransom proceeds on their way to becoming rubles or hryvnia.

The defendant’s conduct falls within the heartland of Title 18, Section 1960(b)(1)(C), which Congress enacted after the September 11 attacks to address nontraditional methods of value transfer that could enable crime and terrorism. See H.R. Rep. 107-250, 54

(noting that under new provision, “[i]t would not be necessary for the Government to show that the business was a storefront or other formal business open to walk-in trade”). The defendant appeared before Your Honor on December 6, 2023 and squarely took responsibility for the crime charged, stating that he knew “that ransomware proceeds and many transactions associated with the Hydra Market were making their way into Bitzlato.” The evidence independently gathered by the government, and discussed in greater detail above, indeed proves that this was true.

The defendant’s sentencing memorandum strains to minimize his culpability, seeking to shrink the conduct here to a regulatory offense and blaming it on the defendant’s customers and colleagues. See Deft. Mem. 14 (portraying defendant’s guilty plea as agreement to “[ac]knowledge that there must have been criminals using the exchange”) ; id. at 10 (purporting to accept responsibility for Bitzlato’s “failing to adequately monitor the activity moving through its platform”); id. at 2 (defendant should have “pushed harder for compliance by the Bitzlato leadership team”). The Defense Memorandum also minimizes the defendant’s role at Bitzlato, depicting him as a lonely voice of dissent with limited involvement or operational control. See Deft. Mem. 15 (boasting that defendant was “persistent” voice for improvement within Bitzlato; lamenting that defendant went on an eight-month bicycle tour).

To be clear: the defendant owned and operated Bitzlato. He sat atop its organizational chart, and at times served as acting CEO. He was deeply involved in its operational details<sup>9</sup> and was repeatedly advised that the company was serving as a major transit point for drug money.

To be sure, the defendant frequently said that he wished to improve compliance standards at Bitzlato, particularly in 2021 and 2022. But those expressions were empty, unmatched by any real action. In February 2022, when the defendant learned that 20% of his company’s transaction volume consisted of illicit funds, he could have and should have closed the company. But he did not, and that is why he is before this Court for sentencing.

The Court should reject the defendant’s effort to minimize his conduct and displace responsibility for his crimes onto his subordinates. Section 1960(b)(1)(C) specifically criminalizes “owning” and “operating” a money laundering business that deals in illicit proceeds—and that is precisely what the defendant did.

For the foregoing reasons, a substantial sentence is warranted in this case.

[REDACTED]

[REDACTED]

---

<sup>9</sup> Indeed, certain of the conversations cited above (such as the defendant’s admission that Bitzlato’s critics were “right about Hydra”) took place during the period when the Defense Memorandum asserts that he was “off the grid” on a bicycle ride. Deft. Mem. 15.

[REDACTED]

[REDACTED]

[REDACTED]

The government further agrees that the defendant himself did not seek specifically to advance the criminal activities whose fruits ran through his exchange. He was *aware* of that activity, and he presided over a chaotic enterprise whose managers had differing views of the criminals using Bitzlato, ranging from acceptance to tacit approval. But the defendant's personal attitude was one of passive disapproval towards that underlying activity. The defendant repeatedly expressed his desire that Bitzlato come into compliance, even though he remained aware over the years that this goal was never reached and that Bitzlato was continuing to process a large volume of illicit transactions, and continued nonetheless to own, direct, operate and profit from Bitzlato.

The defendant accurately notes that Bitzlato generally attempted to respond to requests for information from law enforcement agents, including from U.S. law enforcement. Deft. Mem. 12. However, the quality of Bitzlato's responses often reflected the sparse information it collected from many of its own users. Thus, in one example reviewed by the government, Bitzlato provided a relatively full response to an FBI agent's query, including a copy of the Bitzlato user's passport, along with the user's registration email address. But in another instance, Bitzlato provided only the user ID associated with that user on Telegram, an encrypted messaging application. The accompanying cover letter to the FBI noted that Bitzlato collected "no technical data" regarding the user.

In light of the above, the government respectfully submits that a variance of up to 12 months below the Guidelines sentence of 60 months is appropriate.



C. The Defendant's Incarceration at MDC Does Not Warrant A Downward Variance

The defendant argues that conditions at the Metropolitan Detention Center ("MDC") argue for a lesser sentence. But the defendant's statements about the MDC are generalities, rather than observations about his particular experience at this facility. See generally Deft. Mem. 36-37 (citing news reports). The allegations to which the defendant refers are serious and the government takes them seriously. But the defendant has proffered very little information about his own experience, and the Court's obligation at sentencing is to focus on this particular defendant, not on the MDC generally. See 18 U.S.C. § 3553(a).

Indeed, Judge Chen recently addressed this issue in United States v. Mustapha, a case where defense counsel raised similar arguments at sentencing. Judge Chen expressed skepticism about the relevance of general allegations about MDC, and the Bureau of Prisons generally, in the context of sentencing—as distinct from arguments about the defendant's personal experience:

With respect to the MDC conditions, I should note upfront that I have varied downward based on the conditions at the MDC, with which I am fully familiar. And I am also fully aware of Judge Furman's case and I respect Judge Furman greatly as a judge.

But I am not -- in this regard, I agree with the Government that I'm not going to be convinced by general descriptions of the conditions at the facility or in the BOP system writ large that a variance is warranted for any particular defendant; rather, I am looking at how those conditions have affected the incarceration, the conditions of the incarceration, experienced by this defendant. And there is far less in the sentencing submission about that than there is about the statistics and rather lurid and graphic descriptions of conditions at the MDC and in the BOP system generally, which I am fully familiar with, as I said before.

...

I'm not going to rely on generalized descriptions of conditions at the MDC or elsewhere, as much as I respect Judge Furman's differing opinion on that, because that's not what I think is relevant to sentencing this defendant.

Transcript of Sentencing, Hon. Pamela K. Chen, United States v. Idris Dayo Mustapha, No. 23-cr-440 (E.D.N.Y. May 1, 2024), at 33-34.

D. A Substantial Sentence Will Not Create Unwarranted Disparities

The defendant finally contends that a substantial sentence would create unwarranted sentence disparities as compared to other defendants with similar records. See 18 U.S.C. § 3553(a)(6), Deft. Mem. 38-42.

The defendant first argues that his case should be resolved through a civil fine, describing himself as a "shareholder" being punished for "AML and KYC issues." Deft. Mem.

38. These descriptions undershoot the reality. The defendant is no mere shareholder but a chief executive and majority owner. And Bitzlato did not have “AML issues” – it laundered hundreds of millions of dollars’ worth of illicit funds. The defendant’s conduct is criminal because of his specific and years-long knowledge that Bitzlato was transacting in illicit funds, and indeed had become notorious for processing illicit proceeds. His fellow executive joked about the prospect of being extradited and going to jail. He suggested buying “an island armed to the teeth.” He read of law enforcement crackdowns and wrote to his colleagues: “We’re next.” These are the words of criminals, not legitimate businesspeople. This level of specific knowledge is properly punished by criminal law, as the defendant himself acknowledged in pleading guilty.

The defendant further argues that Binance and its former CEO were “incomparably worse” than him, and that his sentence should therefore be lower than Zhao’s. Deft. Mem. 38-41.

For context, on November 21, 2023, Binance Holdings Limited (“Binance”), the world’s largest cryptocurrency exchange, pleaded guilty to violations related to the Bank Secrecy Act (“BSA”), failure to register as a money transmitting business, and the International Emergency Economic Powers Act (IEEPA). On the same day, Binance’s CEO and founder, Changpeng Zhao, pleaded guilty to an information charging him with failing to maintain an effective anti-money laundering program, in violation of the BSA. Zhao ultimately received a four-month sentence.<sup>10</sup> See Judgment, United States v. Zhao, No. 23-CR-179 (RAJ), ECF. 91 (W.D. Wa. May 1, 2024).

This case is different from Zhao in a number of pertinent ways. First, after the U.S. authorities investigated Binance and learned of its crimes, Binance cooperated extensively with the government for a long period leading up to Zhao’s plea. Second, Zhao, a citizen and resident of the United Arab Emirates, voluntarily flew to the United States and turned himself in to U.S. authorities pursuant to a plea agreement. Moreover, in addition to Zhao’s plea, Binance itself agreed to an aggregate financial penalty of \$4.3 billion, and agreed to retain an independent compliance monitor for three years and remediate its anti-money laundering and sanctions compliance programs. Finally, the crime to which Zhao pled guilty, *i.e.* violating the Bank Secrecy Act, is associated with extremely low sentencing guidelines ranges, and consequently short sentences; the district court in Zhao found that the applicable Guidelines range was ten to 16 months.

None of the above can be said of this defendant. He did not turn himself in, having decided overseas to surrender; rather, he was arrested while vacationing in Florida. As the defendant’s comment about “an island armed to the teeth” suggests, there is no reason to think that he would have voluntarily submitted to arrest. Nor did Bitzlato, like Binance, pay a fine or cooperate with U.S. authorities. And the defendant did not, like Zhao, merely plead guilty to having deficient controls; he pled guilty to owning a company that he knew was transacting in illicit funds. The associated Guidelines range is therefore appropriately higher. As

---

<sup>10</sup> Zhao was sentenced on April 30, 2024, the day after counsel in this case submitted the Defense Memorandum. Accordingly, the Defense Memorandum does not cite the length of Zhao’s sentence in making arguments about sentence disparities.

the Sentencing Commission has recognized, the money laundering Guideline applies to violations of Section 1960(b)(1)(C) “because the essence of this offense is money laundering.” See U.S. Sentencing Comm’n, Amendment 655 cmt. (Nov. 1, 2003), available at <https://www.ussc.gov/guidelines/amendment/655>.

More broadly, and with all due respect to the District Court in Zhao, the sentence in that case was simply too low. Under Zhao’s leadership, Binance enabled an enormous volume of illicit transactions. Notwithstanding Binance’s significant cooperation and Zhao’s self-surrender, a sentence at or above the Guidelines would have been appropriate in that case; indeed, the government sought a 36-month sentence, which would have represented more than double the top of the Guidelines range. United States’ Sentencing Memorandum, United States v. Zhao, No. 23-CR-179 (RAJ), ECF. 78 (W.D. Wa. April 23, 2024), at 2. Here, the government seeks a significant sentence that would nonetheless represent a downward variance from the Guidelines range. No less is warranted to reflect the gravity of the defendant’s conduct.

## VII. Conclusion

For the foregoing reasons, the government respectfully requests that the Court impose a sentence between 48 and 60 months' imprisonment.

Respectfully submitted,

BREON PEACE  
United States Attorney

By: /s/  
Alexander Mindlin  
Artie McConnell  
Assistant U.S. Attorneys  
(718) 254-6433

By: /s/  
Sarah Wolfe  
Trial Attorney, U.S. Department of Justice  
National Cryptocurrency Enforcement Team  
Computer Crime and Intellectual Property  
Section

cc: Clerk of Court (ENV) (By ECF and Email)  
Mark Schamel, Esq. (by ECF and Email)  
United States Probation Officer (By Email)

## EXHIBIT A



